

VIDEO TRANSCRIPT

Video: “Global Privacy and Content Licensing”
Digital Media Licensing Association 2019 Conference

Speakers: 1) Sejal Patel Richbourg, Assistant General Counsel, Intellectual Property and Litigation, Shutterstock, Inc.
2) Nancy E. Wolff, Partner, Cowan, DeBaets, Abrahams & Sheppard LLP

URLs: <https://www.digitalmedialicensing.org/video-library.shtml>
<https://player.vimeo.com/video/390841940>

Sejal Patel Richbourg: 00:05 I'd like to begin my discussion about privacy law by emphasizing that I think there's a little bit of a misconception about who -- what parties privacy laws are sort of aimed at. I think there's this misconception that these laws are sort of more intended for the bigger companies of the world, the Googles and the Facebooks, but really if you take a step back and take a look at what's happening around the world globally with privacy legislation, you begin to see a very different picture.

Sejal Patel Richbourg: 00:37 So, for those of you who are not familiar, in the EU the GDPR was passed in 2016, and that was probably the first major expansive legislation that gave a lot more rights to individuals and how they're able to control and use their own personal information and how companies that they're giving that information to can use that information. So that passed in 2016 and what's happened since then is very telling of a bigger global move towards giving individuals more rights over their personally identifiable information.

Sejal Patel Richbourg: 01:16 In 2017, China and India followed suit. In 2018, Brazil followed suit. For those of us in this room, I think most importantly, California became the first state in the US to pass a privacy law. And then in 2019, which brings us to today, Australia amended their privacy law and 15 other states in the US have also been

active in drafting legislation, and they're at various points in drafting privacy laws related to data protection.

Sejal Patel Richbourg: 01:51

Here's a visual of what that sort of looks like when you're looking at privacy laws and application to the whole globe. Almost 60% of the countries in the world have some sort of data protection or privacy legislation with an additional 10% with pending legislation. So last year, I focused a lot on GDPR and how the EU law would affect all of us in this room, especially if you have customers in those countries or maybe photographers in those countries, but what we're seeing now is that these laws are being adopted all over the world. And so it's becoming increasingly likely that these will affect how we conduct business.

Sejal Patel Richbourg: 02:38

So every country that's adopted one of these laws has done so in different ways, but there's a few provisions that are common to all of these – or mostly applicable to all of these legislations. And one of them is the right to notice and transparency. There's this idea that if something is happening with your data, you should be able to know what that is. The company should be giving notice if something's happening. Individuals are now given increased right to limit and control the usage of their data. There's the right to be forgotten. If you want to have all of your information completely off of a platform, you should be given the right to do that. A lot of these laws allow for that. The right to opt out, the right to data portability, which I'll get into in a second because it really impacts us as businesses that license content. And then of course, the right to correct and remove data from various databases.

Sejal Patel Richbourg: 03:35

So as an individual, I think personally these rights are great. As somebody who signed up for Facebook in college, I'm very grateful that I can now go into my account and delete everything and it will truly be deleted, mostly relating to fashion choices,

nothing terrible. If you go into Facebook, you can actually see that there's a place for you to download all of your data, like anything that you've ever posted or people have posted about you. It's really interesting. But as a business or as a person who is in a role where I have to look at risk mitigation for my business, I'm very conscious of the fact that this now means that we need to be looking at how we allow these rights to be enforced by the individuals whom the information is about.

Sejal Patel Richbourg: 04:29

So GDPR has now been an implementation for a little bit over a year, and I've put up some stats about sort of what that enforcement looks like a year later. The numbers that sort of jump out at me is that there have been close to 300,000 complaints to regulators. There's been more than 400 cross border cases and 89,000 data breach notifications, as well as 56 million Euros paid out in fines.

Sejal Patel Richbourg: 05:02

I think the reason that these numbers are really important to look at is because in Europe, if an individual wants to file a complaint against you, they file a complaint with what's called a DPA, which is an agency that takes a look at the complaint. You're notified as the business that there's been a complaint against you. You don't necessarily know what that complaint is, and then you start to get into, well, this person that filed this complaint was in France, but my business is only in Germany. So which regulatory authority should be looking at this case? And that incurs a lot of legal fees. We're seeing these numbers in Europe right now, but as I showed in the map earlier, these laws are becoming very expansive in terms of global reach. And so it's something that as a business where these laws might apply, it's something to be very conscious of.

Sejal Patel Richbourg: 05:53

So I think the big question is how does this apply to this room? Are content licensors really subject to these privacy laws? That really in the news, we're hearing about more in relation to

Google and Facebook and some of the other bigger companies. There's a few things to sort of look at, and it'll depend on the nature of your own business, but the first is are you taking information that could identify an individual? Some of this information is really obvious. Like you take somebody's name, a photographer's name, or somebody who is depicted an image. You have their name, their address, their email address, things like that. But in our specific space, we have photographs of people, whether that's because we're licensing them commercially and we have model releases on file for them, or whether they're depicted in editorial content, we actually are holding likely a lot of personal data, which makes many of us subject to these regulations.

Sejal Patel Richbourg: 06:53

The second thing to look at is, is the individual that you're transacting with, whether it's a photographer or somebody who is supplying content to you, are they residing in a state if you're in the US or a country where privacy law applies? And also, where are you located? Because depending on the answers to those questions, different laws may apply. One example is if an individual, for example a model, resides in the EU, then the GDPR would apply to you if you're taking their personal information and doing something with it. If a content licensor is located in California, CCPA, which is the California privacy law could apply.

Sejal Patel Richbourg: 07:35

Lastly, you should take a look at whether you're covered by any exemptions. For example, if you're a licensor in California, you're actually only subject to the privacy law in California if you're meeting a certain revenue requirement. I think that law is if you're making gross revenues of \$25 million or more, or if you're earning 50% or more of your revenues from selling data that would apply to you. Those are sort of the three things to look at to see if any of these laws actually apply.

Sejal Patel Richbourg: 08:10

So lastly, I've come up with this very general, high-level checklist for considerations to think about when it comes to privacy law. So the first is take a look at the data that you're taking in, and you might think, oh, I just have like these emails with some names and, you know, whatever information, and it's not a big deal, but actually if you're taking it, you now have obligations related to that information.

Sejal Patel Richbourg: 08:35

A few years ago, Shutterstock was taking, for example, IDs, because we wanted to verify that the people who are giving us content were real people and, you know, to deter fraud and things like that. And then we realized, well, do we really need all of that data? Do we need that to sit somewhere because we're not really doing anything with it. So really taking a look at the purpose of any data that you have on file is really important because once you have that data, then you have obligations that are attendant to having that data.

Sejal Patel Richbourg: 09:05

The second consideration is determine whether the usage is exempt. There's some exemptions in the various laws where they say, you have this personal information, but you need that in order to fulfill contractual obligations. So you might be covered by that and that's something to take a look at. The third consideration is either update your privacy policies, or if you don't have one on your website, strongly consider creating one. There's a really good template for one on the DMLA website, and it's something that you should definitely take a look at because one of the requirements for taking this data in and using it is getting consent from the end subject.

Sejal Patel Richbourg: 09:47

The fourth consideration is looking at your technical ability to handle data requests. If somebody writes into you, let's say a model writes in and they say, I don't want you to be licensing my images, get them off of your site. Like I want them completely gone. You have to make sure that you're able to do that. Where

are your images sitting? Are they stored in a way that's easy for you to figure out where it sits and to remove them and completely remove them in the way that's being requested?

Nancy Wolff: 10:15 Do you have to do that? Or would there be an exemption because there's a business reason to keep model releases because you need them for licensing.

Sejal Patel Richbourg: 10:22 Yeah, and you're right. And it depends on which law.

Nancy Wolff: 10:26 Because you probably gave everyone a heart attack here.

Sejal Patel Richbourg: 10:29 If you're in an area where a privacy law that requires that, that's something that you should ensure. But really, I think the underlying message is taking a look at your technical abilities for handling any of these requests that the laws apply to you. And then lastly determine a process for breach reporting. So, if your business is not of a certain size, you might not have an obligation to let people know that their data has been breached, but especially with laws like the GDPR, there is a 72-hour notification period once you discover a breach that you have to let the people whose data has been breached to let them know that it's happened. If you find that out on a Friday or if that happens on a Friday, you're gone for the weekend. By Monday, Tuesday, you need to send out a breach notification. You're going to be in trouble if there hasn't been some discussion of how to go about and let people know if that's happened.